UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,113	06/20/2003	Amit Raikar	200309309-1	7736

22879 7590 07/06/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/600,113	RAIKAR ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 April 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed April 11, 2007, have been fully considered but they are not persuasive.

2. Claims 1-20 are pending and have been examined.

Response to Amendment

3. Applicant is reminded of the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56.

4. The objections to the drawings are withdrawn.

5. The objections to the disclosure are withdrawn.

6. The provisional Double Patenting rejection (related to copending Application No. 10/627,374) is withdrawn in view of the Terminal Disclaimer filed on 2/07/07. The provisional Double Patenting rejection (related to US Patent No. 7,007,301) is not withdrawn since no Terminal Disclaimer has been filed.

7. The rejection of claim 10 under 35 U.S.C. 112, first paragraph, is withdrawn.

8. The rejection of claims 7-8 and 10 under 35 U.S.C. 112, second paragraph, is withdrawn.

9. Regarding claims 1, 8, and 17, and Applicant's argument that Desai fails to teach different types of intrusion detection sensors, Examiner respectfully submits that Desai's devices are or host diverse intrusion detection sensors, i.e. fig.1 shows events collected at host IDS (17), network IDS, server, etc. are received at collector(20), also paragraphs 86-98 and claims 1-31. **Applicant's arguments are not persuasive.**

Terminal Disclaimer

10. The terminal disclaimer filed on 2/07/07 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of US Application 10/627,374 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Information Disclosure Statement

11. It is noted that no Information Disclosure has been filed in this application, even though the Background section of the Specification discloses multiple vendors provide intrusion detection systems with some of the features claimed (i.e. issuing alerts – claims 2 and 5 – and providing responses to the detected intrusion – claims 1, 3, and others). An IDS stating the prior art Applicant is aware of is respectfully requested.

Double Patenting

12. Claims 1-20 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-19 of Patent 7,007,301. Although the conflicting claims are not identical, they are not patentably distinct from each other because the subject matter claimed in the instant application is fully disclosed in the referenced patent.

13. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

14. The subject matter claimed in the instant application is fully disclosed in the referenced patent and is covered by the patent granted since the referenced patent and the instant application are claiming common subject matter, as follows:

- the instant application discloses an integrated intrusion detection method comprising: gathering information from a plurality of different types of intrusion detection sensors; processing said information, wherein said processing provides a consolidated correlation of said information; assigning a response corresponding to said information; and implementing said response;
- the patent discloses a computer architecture for an intrusion detection system, comprising: a control agent to interface with a management system and to monitor system activity; at least one data gathering component which gathers kernel audit data and syslog data; at least one correlator to interpret and analyzes the kernel audit data and the syslog data using at least one detection template, wherein said at least one correlator uses an event driven correlation using an Event Correlation Services (ECS) engine core, wherein said at least one detection template is selected from the group including: a modification of files/directories template; a chance to log files template; a SetUID files template; a creation of world-writables template; a repeated failed logins template; a repeated failed SU commands template; a race conditions attack template; a buffer overflow attacks template; a modification of another user's file template; a monitor for the start of interactive sessions template; and a monitor logins/logouts template..

15. Claims 1-20 of the instant application are envisioned by Patent 7,007,301's claims 1-19 in that claims 1-19 of the patent contain all the limitations of claims 1-20 of the instant application. Claims 1-20 of the instant application therefore are not patently distinct from the patent claims and as such are unpatentable for obvious-type double patenting.

Claim Rejections - 35 USC § 102

16. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

17. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Desai et al. (US Patent Application Publication 2003/0188189, hereinafter Desai).

Regarding claim 1, Desai teaches an integrated intrusion detection method comprising **(paragraphs 34-39)**:

- gathering information from a plurality of different types of intrusion detection sensors **(paragraphs 44-49)**;
- processing said information, wherein said processing provides a consolidated correlation of said information **(paragraphs 46-54)**;
- assigning a response corresponding to said information **(paragraphs 52-55)**; and

- implementing said response **(paragraphs 63-76)**.

Regarding claim 8, Desai teaches a computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement intrusion detection instructions comprising **(paragraphs 34-39)**:

- a data collection module for receiving information from a plurality of different types of intrusion detection sensors, wherein said information indicates potential security issues **(paragraphs 44-49)**;
- an integration module for integrating said information in a network application management platform **(paragraphs 46-54)**;
- a reaction determination module for determining appropriate response to indication of said potential security issues **(paragraphs 52-55)**; and
- a reaction direction module for directing said response **(paragraphs 63-76)**.

Regarding claim 17, Desai teaches an intrusion detection central system comprising **(paragraphs 34-39)**:

- a bus for communicating information **(paragraphs 44-49)**;
- a processor coupled to said bus, said processor for processing said information including instructions for coordinating security information from a plurality of different intrusion detection sensors **(paragraphs 46-54)**; and

- a memory coupled to said bus, said memory for storing said information, including instructions for coordinating security information from a plurality of different intrusion detection sensors **(paragraphs 63-76)**.

Regarding claims 2 and 9, Desai teaches wherein said information includes intrusion detection alerts **(paragraphs 49-56)**.

Regarding claim 3, Desai teaches centrally tracking information associated with intrusion detection alerts from said plurality of different types of intrusion detection sensors **(paragraphs 45-52)**.

Regarding claim 4, Desai teaches wherein said tracking information associated with intrusion detection includes assigning severity assignments standardized across said plurality of different types of intrusion detection sensors **(paragraphs 51-56)**.

Regarding claim 5, Desai teaches wherein said intrusion detection alerts are correlated based upon various alert attributes **(paragraphs 45-53)**.

Regarding claim 6, Desai teaches wherein said response conforms to an enterprise wide strategy **(paragraphs 56-62)**.

Regarding claim 7, Desai teaches managing said intrusion detection sensors **(paragraphs 41-46)**.

Regarding claim 10, Desai teaches wherein said integration module selects appropriate hooks in an intrusion detection system **(paragraphs 51-57)**.

Regarding claim 11, Desai teaches wherein said data collection module logs alerts from said plurality of different types of intrusion detection sensors **(paragraphs 45-53)**.

Regarding claim 12, Desai teaches wherein said alerts are provided by a simple network management protocol (SNMP), a system log and an application program interface **(paragraphs 42-52)**.

Regarding claim 13, Desai teaches wherein said integration module includes analyzing a plurality of manners in which an alert can be provided and selecting the manner that is the most secure with the least dependencies in a communication path **(paragraphs 66-78)**.

Regarding claim 14, Desai teaches wherein said integration module utilizes a network application management platform to log information **(paragraphs 42-52)**.

Regarding claim 15, Desai teaches wherein: an open view operation simple network management protocol trap is utilized to handle simple network management protocol trap based alerts; an open view operation log file encapsulator handles system log based alerts; and an open view message interceptor handles application program interface propagated alerts with the help of an operation message mechanism **(paragraphs 41-52)**.

Regarding claim 16, Desai teaches wherein a secure open view template configuration is utilized to log information and the one message group is configured for handling intrusion detection system alerts and another message group is configured for handling intrusion detection system errors **(paragraphs 45-52, 75-79)**.

Regarding claim 18, Desai teaches wherein said instructions include security management instructions implemented on a network application management platform **(paragraphs 64-79)**.

Regarding claim 19, Desai teaches a central console for interfacing with said network application management platform **(paragraphs 95-101)**.

Regarding claim 20, Desai teaches wherein said instructions include incident reaction instructions **(paragraphs 66-78)**.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Hackenberger et al. (US Patent Application Publication 2002/0184532) teaches multiple security modules providing alerts, Fischman et al (US Patent Application Publication 2003/0097588) teaches correlating security information from diverse sources for intrusion detection, Bruton, III et al. (US Patent Application Publication 2003/0145225) teaches a centralized intrusion detection system, Scheidell (US Patent Application Publication 2004/0098623) teaches an IDS gathering information from a plurality of different types of intrusion detection sensors; processing said information, wherein said processing provides a consolidated correlation of said information; assigning a response corresponding to said information; and implementing said response.

19. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.
21. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
22. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DGC

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

7,2,07